Claims

1-3. (cancelled)

4. (currently amended) A computer-readable medium containing computer-executable instructions for performing ~~the method of claim 29~~ a method of obtaining a Montgomery product of a first cryptographic parameter X and a second cryptographic parameter Y with respect to a modulus M, wherein X and Y are represented by m bits, the method comprising:

selecting a word length w and a number of words e;

representing the second cryptographic parameter and the modulus M as e words of length w, wherein e is at least 2; and

obtaining an intermediate value of a first word of the Montgomery product based on a product of a word of the second cryptographic parameter, a word of the modulus, and a bit of the first cryptographic parameter.

5. (currently amended) A method for secure communication of a message to a message recipient, the method comprising:

receiving the message from a message sender;

~~for~~ obtaining a Montgomery product of a first cryptographic parameter X and a second cryptographic parameter Y with respect to a modulus M, wherein X and Y are represented by m bits and at least one of the first cryptographic parameter and the second cryptographic parameter is based on the received message, wherein the Montgomery product is obtained by a ~~the~~ method comprising:

selecting a word length w and a number of words e;

representing the second cryptographic parameter and the modulus M as e words of length w, wherein e is at least 2; and

obtaining an intermediate value of a first word of the Montgomery product based on a product of a word of the second cryptographic parameter and a bit of the first cryptographic parameter. ~~parameter; and.~~

6. (original) The method of claim 5, wherein a product of the word length w and the number

of words e such that $w \cdot e \geq m$.

7. (previously presented) The method of claim 5, further comprising obtaining an intermediate value of a second word of the Montgomery product based on a product of a second word of the second cryptographic parameter and a second bit of the first cryptographic parameter in parallel with obtaining the intermediate value of the first word.

8. (previously presented) The method of claim 5, further comprising updating the intermediate value of the first word of the Montgomery product with a contribution from at least one product of a second selected bit of the first cryptographic parameter with at least a second selected word of the second cryptographic parameter.

9. (currently amended) A computer-readable medium containing instructions for performing ~~the method of claim 8~~ a method of obtaining a Montgomery product of a first cryptographic parameter X and a second cryptographic parameter Y with respect to a modulus M, wherein X and Y are represented by m bits, the method comprising:

selecting a word length w and a number of words e;

representing the second cryptographic parameter and the modulus M as e words of length w, wherein e is at least 2;

obtaining an intermediate value of a first word of the Montgomery product based on a product of a word of the second cryptographic parameter and a bit of the first cryptographic parameter; and

updating the intermediate value of the first word of the Montgomery product with a contribution from at least one product of a second selected bit of the first cryptographic parameter with at least a second selected word of the second cryptographic parameter.

10. (currently amended) A computer-readable medium containing instructions for performing ~~the method of claim 5~~ a method of obtaining a Montgomery product of a first cryptographic parameter X and a second cryptographic parameter Y with respect to a modulus M, wherein X and Y are represented by m bits, the method comprising:

selecting a word length w and a number of words e;

representing the second cryptographic parameter and the modulus M as e words of length w, wherein e is at least 2; and

obtaining an intermediate value of a first word of the Montgomery product based on a product of a word of the second cryptographic parameter and a bit of the first cryptographic parameter.

11-16. (cancelled)

17. (currently amended) An apparatus for performing a Montgomery multiplication of a first operand and a second operand with respect to a modulus, the apparatus comprising:

a plurality of processing elements that include inputs for words of the first operand, words of the modulus, an intermediate value of a word of a Montgomery product, and an input for a bit of the second operand; and

a control unit situated and configured to direct words of the first operand, words of the modulus, and bits of the second operand to the processing elements, wherein the processing elements include task processors that receive words of the first operand, words of the modulus, and produce intermediate values of word of a Montgomery product.

18. (original) The apparatus of claim 17, further comprising a data path along which words of the first operand are delivered to the processing elements.

19. (canceled)

20. (currently amended) A circuit for obtaining a Montgomery product of first and second operands with respect to a modulus, the circuit comprising:

at least a first processing element and a second processing element, each of the processing elements including inputs that receive words of the first operand and the modulus, and outputs that deliver values of words of the Montgomery product; and

a data path configured to deliver values of words of the Montgomery product from the first processing element to the second processing element.

21. (original) The circuit of claim 20, further comprising an input for receiving a value associated with a precision of the first and second operands.

22. (original) The circuit of claim 20, wherein the data path is configured to provide a first selected bit of the second operand to the first processing element, and a second selected bit of the second operand to the second processing element.

23. (original) A task processor for obtaining a Montgomery product of a first operand and a second operand with respect to a modulus M, the task processor comprising:

an input configured to receive a bit of the first operand;

an input configured to receive a word of the second operand;

an input configured to receive a word of the modulus;

a computational unit that determines a contribution to a final or intermediate value of a word the Montgomery product based on the received bit of the first operand and the received words of the second operand and the modulus; and

an output configured to supply a final or intermediate value of the word of the Montgomery product.

24. (original) A cryptographic processor, comprising a plurality of task processors as recited in claim 23 and configured to determine a Montgomery product.

25. (original) A cryptographic processor, comprising:

an input for a message; and

an apparatus for obtaining a Montgomery product as recited in claim 17 that produces a Montgomery product based on the message.

26. (currently amended) A smart card, comprising a cryptographic processor configured to determine a Montgomery product of a first cryptographic parameter X and a second cryptographic parameter Y with respect to a modulus M, wherein X and Y are represented by m bits, by ~~the~~ a method ~~of claim 5~~ comprising:

selecting a word length *w* and a number of words *e*;

representing the second cryptographic parameter and the modulus *M* as *e* words of length *w*, wherein *e* is at least 2; and

obtaining an intermediate value of a first word of the Montgomery product based on a product of a word of the second cryptographic parameter and a bit of the first cryptographic parameter.

27. (previously presented) The smart card of claim 26, wherein the first cryptographic parameter and the second cryptographic parameter are equal.

28. (previously presented) The smart card of claim 26, wherein the first cryptographic parameter corresponds to a user authentication code.

29. (previously presented) The method of claim 5, further comprising obtaining the intermediate value of the first word of the Montgomery product based on the product of a word of the second cryptographic parameter, a word of the modulus, and a bit of the first cryptographic parameter.

30. (previously presented) A smart card, comprising a Montgomery multiplication module having a word input configured to receive words of a first cryptographic parameter, a word input configured to receive words of a modulus, and a bit input configured to receive bits of a second cryptographic parameter.